(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 08314805 A

(43) Date of publication of application: 29.11.96

(51) Int. Cl G06F 12/14
G06F 15/00

(21) Application number: 07121853

(22) Date of filing: 19.05.95

(71) Applicant: NEC CORP

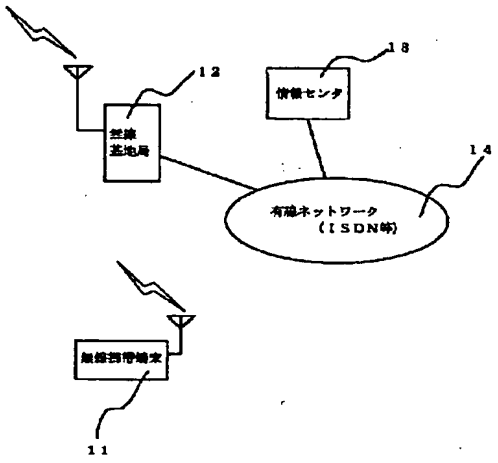
(72) Inventor: ARIGA KENICHI

(54) SYSTEM FOR PREVENTING PORTABLE RADIO TERMINAL FROM BEING ILLEGALLY USED AND METHOD FOR EXECUTING THE SAME

(57) Abstract:

PURPOSE: To prevent a portable radio terminal from being illegally used by providing a means for erasing internal data after the completion of backup copy.

CONSTITUTION: A portable radio terminal 11 judges the illegal use of the terminal and transmits an illegal use report message to an information center 13. At the information center 13, a system data dump request message is transmitted for the backup copy of internal data in the portable radio terminal 11. On the side of the portable radio terminal, the transmission of internal data is started after the system data dump request message was transmitted. These system data of the portable radio terminal 11 are sent every packet as unit and at the information center 13, a reception confirm message is transmitted to the portable radio terminal 11 for every packet. After the completion of backup copy, the information center 13 transmits a system lock request message to the portable radio terminal 11. At the portable radio terminal 11, a system lock complete message is transmitted, the internal data are erased, and the portable radio terminal 11 is turned to be in an unusable state and locked.



ABSTRACT OF THE DISCLOSURE

Purpose

The invention aims at preventing a radio portable terminal lost or stolen from being used fraudulently by any one other than its owner, thus improving security.

Configuration

The invention has such a configuration that if a password for activating a radio portable terminal is input fraudulently a regulated number of times, an information center managing the radio portable terminal is automatically notified of fraudulent use thereof, whereupon the radio portable terminal encrypts data stored therein and dumps it to the information center, where the encrypted data is copied as back-up data and then all deleted in the radio portable terminal.

[0007]

Means for Solving the Problems

To achieve the above-mentioned object, a first embodiment of the invention provides a system for preventing fraudulent use of a radio portable terminal registered in an information center to thereby receive a service therefrom, including an input means provided at the radio portable terminal for inputting a password, a transmission means provided to the radio portable terminal for notifying the information center of a fact that the password is input fraudulently a predetermined number

of times, a means for creating a backup copy of internal data of the radio portable terminal based on an instruction from the information center, and a means for erasing the internal data after its backup copy is created.

[0008]

A second embodiment of the invention provides a system for preventing fraudulent use of a radio portable terminal registered in the information center to thereby receive a service therefrom, including an input means provided to the radio portable terminal for inputting a password, a detection means provided to the information center for detecting that the password is input fraudulently a predetermined number of times, a means for creating a backup copy of internal data of the radio portable terminal in a memory of the information center based on an instruction therefrom, and a means for erasing the internal data after its backup copy is created.

[0009]

A third embodiment of the invention provides a method for preventing fraudulent use of a radio portable terminal registered in the information center to thereby receive a service therefrom, including the steps of inputting a password through an input means of the radio portable terminal, notifying the information center of a fact that the password is input fraudulently input a predetermined number of times, creating a backup copy of internal data of the radio portable terminal in a memory of the information center based on an instruction therefrom, and erasing the internal data after the backup copy

is created.

[0010]

A fourth embodiment of the invention provides a method for preventing fraudulent use of a radio portable terminal registered in the information center to thereby receive a service therefrom, including the steps of inputting a password through an input means of the radio portable terminal, detecting, at the information center, a fact that the password is input fraudulently a predetermined number of times, creating a backup copy of internal data of the radio portable terminal in a memory of the information center based on an instruction therefrom, and erasing the internal data after the backup copy is created.

[0011]

In addition to the four basic embodiments described above, the invention gives the following embodiments also. First, the radio portable terminal fraudulent use preventing method according to the third or fourth embodiment is provided in which when a backup copy is created, a message requesting for dumping of system data transmitted from the information center to the radio portable terminal contains key data required to encrypt the system data of the radio portable terminal.

[0012]

Also, the radio portable terminal fraudulent use preventing method according to the third or fourth embodiment is provided in which the internal data of the radio portable terminal is encrypted using an encryption key sent from the information center.

[0013]

Further, the system data of the radio portable terminal is sent in packet units, in response to which the information center transmits a reception confirmation message for each packet.

[0014]

Actions

If some one other than the owner of a radio portable terminal uses it and, to use it, inputs a password fraudulently a predetermined number of times, the radio portable terminal posts fraudulent use to the information center, which in turn backs up the internal data of this terminal based on this posting and then transmits to this terminal a request for erasing its internal data, thus disabling this terminal. Thus, a stolen radio portable terminal can be prevented from being used fraudulently.

[0015]

Embodiments

The following will describe in further details the preferred embodiments of the invention with reference to the drawings. FIG. 1 is an overall configuration diagram for showing a radio portable terminal system used in the invention, FIG. 2 is a block diagram for showing a hardware configuration of the radio portable terminal used in the invention, FIG. 3 is a sequence diagram for showing operations of the first embodiment of the invention, and FIG. 4 is a sequence diagram for showing operations of the second embodiment of the

invention.

[0016]

First, the hardware configuration of a radio portable terminal used in the invention is described with reference to FIG. 2.

[0017]

The radio portable terminal includes a CPU21 for controlling the system as a whole, a ROM24 storing a control program etc., a work RAM22 used by the control program, a data accumulating RAM23 for accumulating therein such individual data as addresses and schedules, an indicator 25 for displaying information and operations, an input device 26 for inputting data, and a radio module 27 for controlling wireless communication.

[0018]

The data input through the input device 26 is accumulated in the accumulating RAM23.

[0019]

Since the data accumulating RAM23 is generally backed up by a battery, its contents do not disappear even when its power is turned OFF. To wirelessly transmit data, it is sent from the RAMs22 and 23 and the ROM24 through the system bus to the radio module 27 for transmission.

[0020]

Next, the overall configuration of the radio portable terminal system is described with reference to FIG. 1.

[0021]

Suppose that some one other than the owner is trying to use a radio portable terminal 11 fraudulently. The radio portable terminal 11 is registered in and managed by an information center 13 so that it may be accessed through a radio base station 19 from the information center 13 connected to a cable network 14.

[0022]

The following will describe operations of the first embodiment of the invention with reference to the sequence diagram of FIG. 3.

[0023]

Suppose that some one other than the owner, in an attempt to use the radio portable terminal 11, tried fraudulently to enter its password and failed in it a system-regulated number of times. In this case, the radio portable terminal 11 decides this trial as fraudulent use of the terminal and transmits a fraudulent-use notification message to the information center 13 to notify it of that [301].

The information center 13, when received the fraudulent-use notification message, transmits a system-data dump request message in order to copy backup data of the internal data of the radio portable terminal 11 [302].

To this message is added key data required to encrypt the system data of the radio portable terminal 11. Upon reception of this message, the radio portable terminal transmits a system-data dump start message and then starts transmitting its internal data [303].

The internal data is encrypted using an encryption key sent from the information center 13 so that the data may not be intercepted illegally.

[0024]

The system data of the radio portable terminal 11 is sent in packet units to the information center 13, which in turn transmits a reception confirmation message to the radio portable terminal 11 for each packet received [304].

When having copied the backup data, the information center 13 transmits a system-lock request message to the radio portable terminal 11. The radio portable terminal 11, upon reception of this message, transmits a system-lock completion message to then erase the internal data and locks itself in an unusable state [305-306].

FIG. 4 shows a sequence diagram of operations according to the second embodiment of the invention in a case where the side of the information center detects that the password has been input fraudulently a system-regulated number of times. In this second embodiment, use of the radio portable terminal 11 is decided at the information center 13 on whether it is fraudulent, so that it is unnecessary, in contrast to the above-mentioned first embodiment, for the radio portable terminal 11 to transmit a fraudulent-use notification message to the information center 13. The other operations are the same as those of the first embodiment and so omitted in description.

[0025]

Effects of the Invention

As described above, by the radio portable terminal fraudulent-use preventing method by the invention, if some one other than the owner of a radio portable terminal happens to acquire it and, to use it, inputs an incorrect password a few times, the internal data of the radio portable terminal is erased and the terminal is put into a locked state, to thereby prevent him from accessing the radio network or referencing such internal data as addresses after the radio portable terminal is lost and stolen, thus preserving its security. Also, the internal data, prior to being erased, is copied as backup data in a memory of the information center which manages the terminal, thus facilitating recovery by the illegal user of the terminal when he reuses it.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平8－314805

(43)公開日　平成８年(1996)11月29日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	12/14	３２０		Ｇ０６Ｆ	12/14	３２０Ｄ
	15/00	３３０	9364－5Ｌ		' 15/00	３３０Ｃ

審査請求　有　　請求項の数７　ＯＬ　（全 5 頁）

(21)出願番号　特願平7－121853

(22)出願日　平成７年(1995)５月19日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　有賀　健一
東京都港区芝五丁目７番１号　日本電気株式会社内

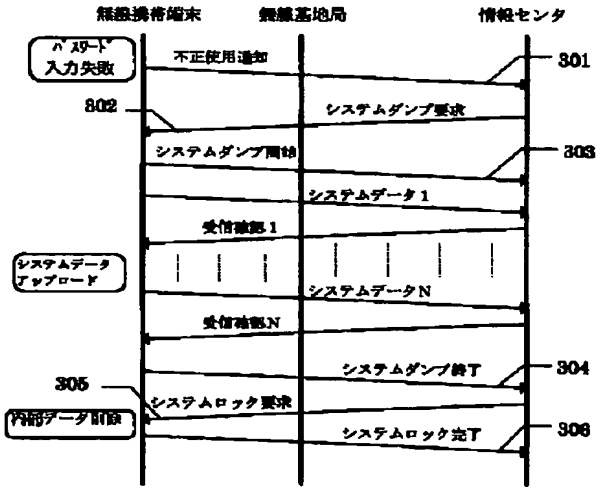
(74)代理人　弁理士　鈴木　弘男

(54)【発明の名称】　無線携帯端末不正使用防止システム及びその実施方法

(57)【要約】

【目的】　本発明の目的は、紛失したか、または盗難された無線携帯端末が所有者以外の者によって力を不正使用されることを防止して、セキュリティの向上を図ることにある。

【構成】　本発明は、無線携帯端末を操作開始するためのパスワードを規定回数失敗すると、無線携帯端末を管理している情報センタに不正使用されている旨を自動的に通知し、それを受けて無線携帯端末は内部データを暗号化して情報センタにダンプを行い、情報センタにおけるバックアップコピーのとり終り後に無線携帯端末の内部データをすべて削除するように構成されている。



1

【特許請求の範囲】

【請求項１】　情報センタに登録されてそのサービスを受けている無線携帯端末の不正使用防止システムであって、

前記無線携帯端末に設けられた、パスワード入力を行うための入力手段と、

該パスワード入力が所定回数誤って行われたことを前記情報センタに通知するように無線携帯端末に設けられた送信手段と、

前記情報センタからの指示に基づいて、前記無線携帯端末の内部データのバックアップコピーを前記情報センタ内の記憶装置にとる手段と、

該バックアップコピーのとり終り後に該内部データを消去する手段と、を具備することを特徴とする無線携帯端末不正使用防止システム。

【請求項２】　情報センタに登録されてそのサービスを受けている無線携帯端末の不正使用防止システムであって、

前記無線携帯端末に設けられた、パスワード入力を行うための入力手段と、

該パスワード入力が所定回数誤って行われたことを検出するように前記情報センタに設けられた検出手段と、

前記情報センタからの指示に基づいて、前記無線携帯端末の内部データのバックアップコピーを前記情報センタ内の記憶装置にとる手段と、

該バックアップコピーのとり終り後に該内部データを消去する手段と、を具備することを特徴とする無線携帯端末不正使用防止システム。

【請求項３】　情報センタに登録されてそのサービスを受けている無線携帯端末の不正使用防止方法であって、

前記無線携帯端末の入力手段を介してパスワード入力を行うことと、

該パスワード入力が所定回数誤って行われたことを前記情報センタに通知することと、

前記情報センタからの指示に基づいて、前記無線携帯端末の内部データのバックアップコピーを前記情報センタ内の記憶装置にとることと、

該バックアップコピーのとり終り後に該内部データを消去すること、の各ステップからなることを特徴とする無線携帯端末不正使用防止方法。

【請求項４】　情報センタに登録されてそのサービスを受けている無線携帯端末の不正使用防止方法であって、

前記無線携帯端末の入力手段を介してパスワード入力を行うことと、

該パスワード入力が所定回数誤って行われたことを情報センタにおいて検出することと、

前記情報センタからの指示に基づいて、前記無線携帯端末の内部データのバックアップコピーを前記情報センタ内の記憶装置にとることと、

該バックアップコピーのとり終り後に該内部データを消

2

去すること、の各ステップからなることを特徴とする無線携帯端末不正使用防止方法。

【請求項５】　前記バックアップコピーをとる際に、前記情報センタから前記無線携帯端末に送信されるシステムデータダンプ要求メッセージが前記無線携帯端末のシステムデータを暗号化するためのキーデータを含むことを特徴とする請求項３および請求項４のいずれかに記載の無線携帯端末不正使用防止方法。

【請求項６】　前記無線携帯端末の内部データが前記情報センタから送られてくる暗号キーを用いて暗号化されることを特徴とする請求項３および請求項４のいずれかに記載の無線携帯端末不正使用防止方法。

【請求項７】　前記無線携帯端末のシステムデータがパケット単位で送られると共に、前記情報センタにおいてはパケット毎に受信確認メッセージが送信されることを特徴とする請求項５に記載の無線携帯端末不正使用防止方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は無線携帯端末における不正使用に対するネットワークを介した防止システムとその実施方法に関する。

【０００２】

【従来の技術】近年、無線携帯端末が世の中に普及しつつあるが、無線携帯端末のセキュリティ確保についてはまだまだ発展途上段階にある。従来の無線携帯端末の中には紛失したり盗難にあったりした場合のセキュリティを確保するために、パスワードを設定しそれを起動時に入力させるようになっているものがある（例えば、特開昭６３－１０２６０号公報参照）。また、ＩＣカードに個人のパスワードを記憶しておき、そのＩＣカードを端末に入れることによってホストに接続するようなものがある（例えば、特開平２－２２６４５６号公報参照）。

【０００３】特開平２－２２６４５６号公報には、ユーザが入力する第１の識別コードと、このユーザが利用するカードに記録されている第２の識別コードとの対が、ホストに設けられている識別コードテーブルと一致したときのみ使用可能にする計算機システムについて記載されている。

【０００４】一方、特開平２－１１２０５３号公報には、外部から供給されるパスワードと内部に保有するパスワードとの一致／不一致を判定し、判定結果が一致する場合に内部に保有するパスワードを所定の規則に従って更新することにより、セキュリティの向上を図るデータ処理方法について記載されている。

【０００５】

【発明が解決しようとする課題】無線携帯端末を紛失または盗難され、その端末を第三者が取得して不正に使用することを試みた場合、パスワード機能がなければ自由に無線ネットワークへのアクセスや住所録などの内部デ

ータの参照が可能である。またパスワード機能があっても、無制限にパスワード入力を繰り返すことが可能ならば、何らかの手段によってパスワードを解読され、不正使用を防止することはできない。

【０００６】

【発明の目的】本発明の目的は、盗難に遭ったか、または紛失した無線携帯端末が所有者以外の者によって不正使用されることを防止して、セキュリティの向上を図るようにした無線携帯端末不正使用防止システムおよびその実施方法を提供することである。

【０００７】

【課題を解決するための手段】上記目的を達成するために、本発明の第１態様によれば、情報センタに登録されてそのサービスを受けている無線携帯端末の不正使用防止システムであって、前記無線携帯端末に設けられた、パスワード入力を行うための入力手段と、該パスワード入力が所定回数誤って行われたことを前記情報センタに通知するように無線携帯端末に設けられた送信手段と、前記情報センタからの指示に基づいて、前記無線携帯端末の内部データのバックアップコピーを前記情報センタ内の記憶装置にとる手段と、該バックアップコピーのとり終り後に該内部データを消去する手段とを具備することを特徴とする無線携帯端末不正使用防止システムが提供される。

【０００８】本発明の第２態様によれば、情報センタに登録されてそのサービスを受けている無線携帯端末の不正使用防止システムであって、前記無線携帯端末に設けられた、パスワード入力を行うための入力手段と、該パスワード入力が所定回数誤って行われたことを検出するように前記情報センタに設けられた検出手段と、前記情報センタからの指示に基づいて、前記無線携帯端末の内部データのバックアップコピーを前記情報センタ内の記憶装置にとる手段と、該バックアップコピーのとり終り後に該内部データを消去する手段とを具備することを特徴とする無線携帯端末不正使用防止システムが提供される。

【０００９】本発明の第３態様によれば、情報センタに登録されてそのサービスを受けている無線携帯端末の不正使用防止方法であって、前記無線携帯端末の入力手段を介してパスワード入力を行うことと、該パスワード入力が所定回数誤って行われたことを前記情報センタに通知することと、前記情報センタからの指示に基づいて、前記無線携帯端末の内部データのバックアップコピーを前記情報センタ内の記憶装置にとることと、該バックアップコピーのとり終り後に該内部データを消去することの各ステップからなることを特徴とする無線携帯端末不正使用防止方法が提供される。

【００１０】本発明の第４態様によれば、情報センタに登録されてそのサービスを受けている無線携帯端末の不正使用防止方法であって、前記無線携帯端末の入力手段

を介してパスワード入力を行うことと、該パスワード入力が所定回数誤って行われたことを情報センタにおいて検出することと、前記情報センタからの指示に基づいて、前記無線携帯端末の内部データのバックアップコピーを前記情報センタ内の記憶装置にとることと、該バックアップコピーのとり終り後に該内部データを消去することの各ステップからなることを特徴とする無線携帯端末不正使用防止方法が提供される。

【００１１】以上４個の基本態様に加えて、本発明は次のような実施態様を有する。まず、上記第３および第４態様のいずれかに記載の無線携帯端末不正使用防止方法において、バックアップコピーをとる際に、情報センタから無線携帯端末に送信されるシステムデータダンプ要求メッセージが無線携帯端末のシステムデータを暗号化するためのキーデータを含む。

【００１２】また、上記第３および第４態様のいずれかに記載の無線携帯端末不正使用防止方法において、無線携帯端末の内部データが情報センタから送られてくる暗号キーを用いて暗号化される。

【００１３】さらに、無線携帯端末のシステムデータはパケット単位で送られると共に、前記情報センタにおいてはパケット毎に受信確認メッセージが送信される。

【００１４】

【作用】所有者以外の第三者が無線携帯端末を使用してこの無線携帯端末を使用するためのパスワードを予め決められた回数以上謝ると、無線携帯端末は情報センタに対して不正使用の通知を行ない、この通知により情報センタは端末内部のデータバックアップをとった後に端末の内部データを消去する要求を無線携帯端末に送信し、無線携帯端末を使用不可の状態にする。これによって盗難された無線携帯端末の不正使用を防止することができる。

【００１５】

【実施例】以下、本発明を添付の図面に示す好ましい実施例に関連してさらに詳細に説明する。図１は本発明に用いられる無線携帯端末システムの全体構成図であり、図２は本発明に用いられる無線携帯端末のハードウェア構成を示すブロック図であり、図３は本発明の第１実施例の動作を示すシーケンス図であり、図４は本発明の第２実施例の動作を示すシーケンス図である。

【００１６】まず、図２を参照して本発明に用いられる無線携帯端末のハードウェア構成が説明される。

【００１７】無線携帯端末は、システム全体を制御するＣＰＵ２１、制御プログラム等が蓄積されているＲＯＭ２４、制御プログラムが使用するワーク用ＲＡＭ２２、住所録やスケジュールなどの個人データが蓄積されているデータ蓄積用ＲＡＭ２３、情報や操作を表示するための表示器２５、データを入力するための入力装置２６、無線の制御を行なう無線モジュール２７で構成されている。

5

【００１８】入力装置２６で入力されたデータはデータ蓄積用ＲＡＭ２３に蓄積される。

【００１９】一般的にデータ蓄積用ＲＡＭ２３は電池でバックアップされているために、電源を落としても消去されることはない。無線でデータの送信を行なう場合には、ＲＡＭ２２、２３、ＲＯＭ２４からシステムバスを通じて、無線モジュール２７にデータが送られ、これによってデータの送信が行われる。

【００２０】次に無線携帯端末システムの全体構成を図１を用いて説明する。

【００２１】いま、所有者以外の第三者が不正使用をしようとしている無線携帯端末を１１とする。無線携帯端末１１は情報センタ１３に登録、管理されていて、有線ネットワーク１４に接続されている情報センタ１３に対して無線基地局１９を通じてアクセスできるようになっている。

【００２２】図３のシーケンス図を用いて本発明の第１実施例の動作を説明する。

【００２３】今、所有者以外の第三者が無線携帯端末１１を不正に用いようとして、パスワード入力を試み、システムで規定されている回数の入力誤りを起こしたとする。この時、無線携帯端末１１は、端末が不正使用されようとしていると判断して、これを情報センタ１３に通知するために不正使用通知メッセージを情報センタ１３に送信する。［３０１］

不正使用通知メッセージを受信した情報センタ１３では、無線携帯端末１１の内部データのバックアップコピーをとるためにシステムデータダンプ要求メッセージを送信する。［３０２］

このメッセージには無線携帯端末１１のシステムデータを暗号化するためのキーデータを付加する。無線携帯端末側でこのメッセージを受信すると、システムデータダンプ開始メッセージを送信した後、内部データの送信を開始する。［３０３］

内部データは無線を通じて不正に取り込まれないように、情報センタ１３から送られてきた暗号キーを用いて、暗号化される。

【００２４】無線携帯端末１１のシステムデータはパケット単位で送られ、情報センタ１３ではパケット毎に受信確認メッセージを無線携帯端末１１に送信する。［３０４］

情報センタ１３は、バックアップコピーのとり終り後に、システムロック要求メッセージを無線携帯端末１１に送信する。無線携帯端末１１ではこのメッセージを受信後にシステムロック完了メッセージを送信して、内部

6

データを消去して無線携帯端末を使用不可の状態にしてロックする。［３０５－３０６］

本発明の第２実施例として、システムで規定された回数だけパスワードの入力誤りを起こしたことを情報センタで検出する場合の動作が図４のシーケンス図に示される。この第２実施例では、無線携帯端末１１の不正使用が情報センタ１３において判断されるので、前述の第１実施例における無線携帯端末１１から情報センタ１３への不正使用通知メッセージの送信動作は不要になる。それ以外は第１実施例と同じ動作が行われるので、重複を避けるためにそれらの説明を省略する。

【００２５】

【発明の効果】以上説明したように、本発明の無線携帯端末不正使用防止方法は、第三者によって取得された無線携帯端末を不正に用いようとして、誤ったパスワード入力を数回試みると無線携帯端末内部のデータが消去して端末をロック状態にするために、無線携帯端末を紛失したり盗難にあったりした後に、第三者が無線ネットワークへのアクセスや住所録などの内部データを参照することができなくなり、無線携帯端末のセキュリティが保たれる。また内部データを消去する前にデータのバックアップコピーを管理先の情報センタに備えられた記憶装置にとって置くので、正規の持ち主によってなされる再使用時における復旧が容易である。

【図面の簡単な説明】

【図１】本発明で用いられる無線携帯端末システムの全体構成図である。

【図２】本発明で用いられる無線携帯端末のハードウェア構成を示すブロック図である。

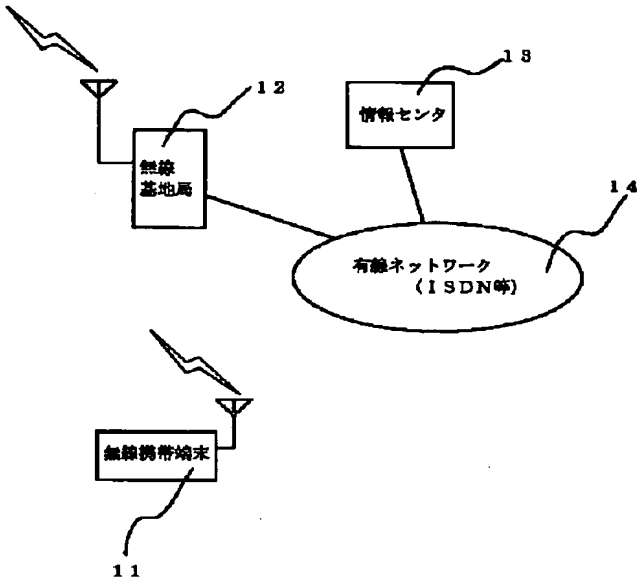
【図３】本発明の第１実施例の動作を示すシーケンス図である。

【図４】本発明の第２実施例の動作を示すシーケンス図である。

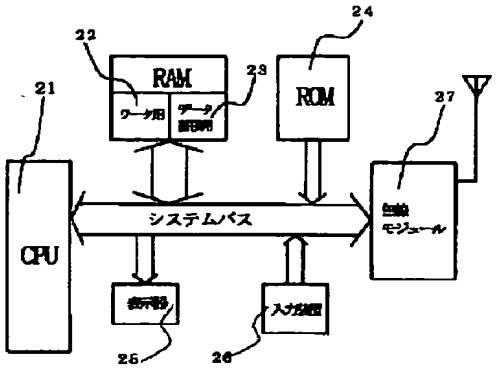
【符号の説明】

１１　無線携帯端末
１２　無線基地局
１３　情報センタ
１４　有線ネットワーク
２１　ＣＰＵ
２２　ワーク用ＲＡＭ
２３　データ蓄積用ＲＡＭ
２４　ＲＯＭ
２５　表示器
２６　入力装置
２７　無線モジュール

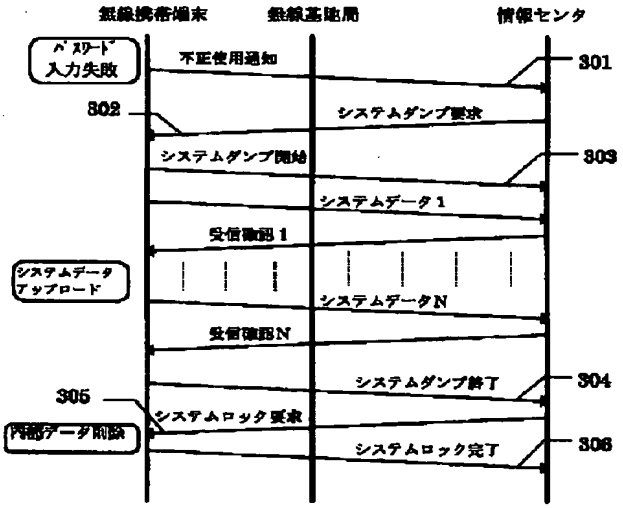
【図１】


情報センタ
13
12
無線
基地局
14
有線ネットワーク
（ＩＳＤＮ等）
無線携帯端末
11

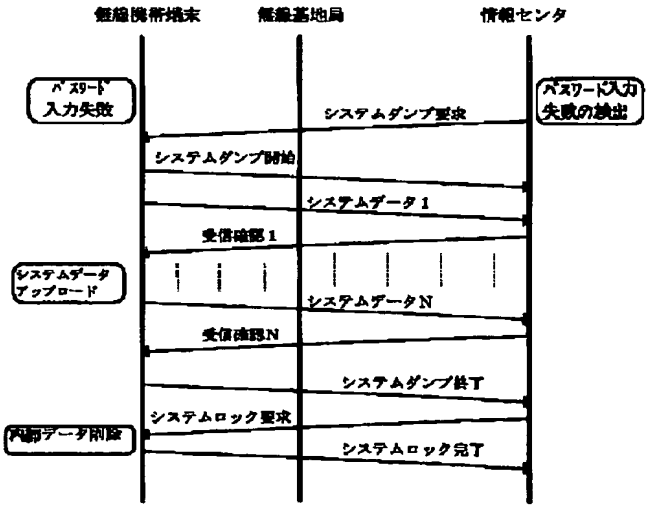
【図２】


22
RAM
23
24
ROM
21
27
CPU
システムバス
無線
モジュール
25
26

【図３】


無線携帯端末
無線基地局
情報センタ
ﾊﾟｽﾜｰﾄﾞ
入力失敗
不正使用通知
301
302
システムダンプ要求
システムダンプ開始
303
システムデータ１
受信確認１
システムデータ
アップロード
システムデータN
受信確認N
システムダンプ終了
304
305
システムロック要求
内部データ削除
システムロック完了
306

【図４】


無線携帯端末
無線基地局
情報センタ
ﾊﾟｽﾜｰﾄﾞ
入力失敗
システムダンプ要求
パスワード入力
失敗の検出
システムダンプ開始
システムデータ１
受信確認１
システムデータ
アップロード
システムデータN
受信確認N
システムダンプ終了
システムロック要求
内部データ削除
システムロック完了